

Abstract of the Disclosure

An AES encryption processor is provided for reducing hardware with improved throughput. The processor is composed of a selector unit selecting an element of a state in response to
5 row and column indices, a S-box for obtaining a substitution value with said selected element used as an index, a coefficient table providing first to fourth coefficients in response to said row index, first to fourth Galois field
10 multiplexers respectively computing first to fourth products, which are obtained by multiplication of said substitution value with first to fourth coefficients, respectively, and an accumulator which accumulates the first to
15 fourth products to develop first to fourth elements of a designated column of a resultant state.